WHAT IS CLAIMED IS:

1. A remotely accessible secure cryptographic system for storing a plurality of private cryptographic keys to be associated with a plurality of users, wherein the cryptographic system associates each of the plurality of users with one or more different keys from the plurality of private cryptographic keys and performs cryptographic functions for each user using the associated one or more different keys without releasing the plurality of private cryptographic keys to the users, the cryptographic system comprising:

a depository system having at least one server which stores a plurality of private cryptographic keys and a plurality of enrollment authentication data, wherein each enrollment authentication data identifies one of multiple users and each of the multiple users is associated with one or more different keys from the plurality of private cryptographic keys;

an authentication engine which compares authentication data received by one of the multiple users to enrollment authentication data corresponding to the one of multiple users and received from the depository system, thereby producing an authentication result;

a cryptographic engine which, when the authentication result indicates proper identification of the one of the multiple users, performs cryptographic functions on behalf of the one of the multiple users using the associated one or more different keys received from the depository system; and

a transaction engine connected to route data from the multiple users to the depository server system, the authentication engine, and the cryptographic engine.

2. A remotely accessible secure cryptographic system, comprising:

a depository system having at least one server which stores at least one private key and a plurality of enrollment authentication data, wherein each enrollment authentication data identifies one of multiple users;

an authentication engine which compares authentication data received by one of the multiple users to enrollment authentication data corresponding to the one of multiple users and received from the depository system, thereby producing an authentication result;

a cryptographic engine which, when the authentication result indicates proper identification of the one of the multiple users, performs cryptographic functions on behalf of the one of the multiple users using at least said private key received from the depository system; and

a transaction engine connected to route data from the multiple users to the depository server system, the authentication engine, and the cryptographic engine.

3. The cryptographic system of Claim 2, wherein the depository system further comprises a plurality of data storage facilities, each data storage facility having at least one server storing a substantially randomized portion of the private key and a substantially randomized portion of the plurality of enrollment authentication data.

4. The cryptographic system of Claim 3, wherein each substantially randomized portion is individually undecipherable.

5. The cryptographic system of Claim 2, wherein the enrollment authentication data includes biometric data.

6. The cryptographic system of Claim 5, wherein the biometric data includes finger print patterns.

7. The cryptographic system of Claim 2, wherein the at least one private key corresponds to the secure cryptographic system.

8. The cryptographic system of Claim 2, wherein the at least one private key corresponds to the one of the multiple users.

9. The trust engine of Claim 2, wherein the cryptographic functions comprise one of digital signing, encryption, and decryption.

10. A method of facilitating cryptographic functions, the method comprising:

associating a user from multiple users with one or more keys from a plurality of private cryptographic keys stored on a secure server;

receiving authentication data from the user;

comparing the authentication data to authentication data corresponding to the user, thereby verifying the identity of the user; and

utilizing the one or more keys to perform cryptographic functions without releasing the one or more keys to the user.

11. The method of Claim 10, wherein the authentication data corresponding to the user was acquired prior to the step of receiving authentication data from the user.

12. The method of Claim 10, further comprising receiving a hash of a message or document.

13. The method of Claim 12, further comprising archiving the hash.

14. An authentication system for uniquely identifying a user through secure storage of the user's enrollment authentication data, the authentication system comprising:

a plurality of data storage facilities, wherein each data storage facility includes a computer accessible storage medium which stores one of portions of enrollment authentication data; and

an authentication engine which communicates with the plurality of data storage facilities and comprises

a data splitting module which operates on the enrollment authentication data to create portions,

a data assembling module which processes the portions from at least two of the data storage facilities to assemble the enrollment authentication data, and

a data comparator module which receives current authentication data from a user and compares the current authentication data with the assembled enrollment authentication data to determine whether the user has been uniquely identified.

15. The authentication system of Claim 14, wherein the portions are not individually decipherable.

16. The authentication system of Claim 14, wherein the each data storage facility is logically separated from any other data storage facility.

17. The authentication system of Claim 14, wherein the each data storage facility is physically separated from any other data storage facility.

18. The authentication system of Claim 14, further comprising a cryptographic engine which, upon the unique identification of the user by the authentication engine, provides cryptographic functionality to the user.

19. The authentication system of Claim 14, wherein the plurality of data storage facilities comprises at least one secure server.

20. The authentication system of Claim 14, wherein unique identification of the user by the authentication engine provides the user authorization to gain access to or to operate one or more systems.

21. The authentication system of Claim 20, wherein the one or more systems include one or more electronic devices.

22. The authentication system of Claim 20, wherein the one or more systems include one or more computer software systems.

23. The authentication system of Claim 20, wherein the one or more systems include one or more consumer electronics.

24. The authentication system of Claim 23, wherein the one or more consumer electronics includes a cellular phone.

25. The authentication system of Claim 20, wherein the one or more systems include one or more cryptographic systems.

26. The authentication system of Claim 20, wherein the one or more systems include one or more physical locations.

27. The authentication system of Claim 14, wherein at least one of the data storage facilities stores at least some of sensitive data, wherein the at least one of the data storage facilities serves the sensitive data when the authentication engine indicates that the user has been uniquely identified.

28. The authentication system of Claim 14, further comprising a data vault which stores sensitive data, wherein the data vault serves the sensitive data when the authentication engine indicates that the user has been uniquely identified.

29. The authentication system of Claim 14, wherein the authentication system outputs an indication of whether the user has been uniquely identified.

30. A cryptographic system, comprising:

a plurality of data storage facilities, wherein each data storage facility includes a computer accessible storage medium which stores one of portions of cryptographic keys; and

a cryptographic engine which communicates with the plurality of data storage facilities and comprises

a data splitting module which operate on the cryptographic keys to create portions,

a data assembling module which processes the portions from at least two of the data storage facilities to assemble the cryptographic keys, and

a cryptographic handling module which receives the assembled cryptographic keys and performs cryptographic functions therewith.

31. The cryptographic system of Claim 30, wherein the portions are not individually decipherable.

32. The cryptographic system of Claim 30, wherein the each data storage facility is logically separated from any other data storage facility.

33. The cryptographic system of Claim 30, wherein the each data storage facility is physically separated from any other data storage facility.

34. The cryptographic system of Claim 30, further comprising an authentication engine which, before the cryptographic functionality may be employed on behalf of a user, uniquely identifies the user.

35. The cryptographic system of Claim 30, wherein the plurality of data storage facilities comprises at least one secure server.

36. A method of storing authentication data in geographically remote secure data storage facilities thereby protecting the authentication data against comprise of any individual data storage facility, the method comprising:

receiving authentication data at a trust engine;

combining at the trust engine the authentication data with a first substantially random value to form a first combined value;

combining the authentication data with a second substantially random value to form a second combined value;

creating a first pairing of the first substantially random value with the second combined value;

creating a second pairing of the first substantially random value with the second substantially random value;

storing the first pairing in a first secure data storage facility; and

storing the second pairing in a second secure data storage facility remote from the first secure data storage facility.

37. A method of storing authentication data comprising:

receiving authentication data;

combining the authentication data with a first set of bits to form a second set of bits;

combining the authentication data with a third set of bits to form a fourth set of bits;

creating a first pairing of the first set of bits with the third set of bits;

creating a second pairing of the first set of bits with the fourth set of bits;

storing one of the first and second pairings in a first computer accessible storage medium; and

storing the other of the first and second pairings in a second computer accessible storage medium.

38. The method of Claim 37, wherein at least one of the first and second computer accessible storage mediums comprises at least one server.

39. The method of Claim 37, wherein the first computer accessible storage medium is geographically remote from the second computer accessible storage medium.

40. The method of Claim 37, wherein the matching of one of the first and second pairings with one of the first and second computer accessible storage mediums is substantially random.

41. The method of Claim 37, wherein at least one of the first and third sets of bits are substantially random.

42. The method of Claim 37, wherein at least one of the first and third sets of bits comprises a bit length equal to a bit length of the sensitive data.

43. The method of Claim 37, wherein both the first and second pairings are needed to reassemble the data.

44. The method of Claim 37, further comprising:

creating a third pairing of the second set of bits with the third set of bits;

creating a fourth pairing of the second set of bits with the fourth set of bits;

storing one of the third and fourth pairings in a third computer accessible storage medium; and

storing the other of the third and fourth pairings in a fourth computer accessible storage medium.

45. A method of storing cryptographic data in geographically remote secure data storage facilities thereby protecting the cryptographic data against comprise of any individual data storage facility, the method comprising:

receiving cryptographic data at a trust engine;

combining at the trust engine the cryptographic data with a first substantially random value to form a first combined value;

combining the cryptographic data with a second substantially random value to form a second combined value;

creating a first pairing of the first substantially random value with the second combined value;

creating a second pairing of the first substantially random value with the second substantially random value;

storing the first pairing in a first secure data storage facility; and

storing the second pairing in a secure second data storage facility remote from the first secure data storage facility.

46. A method of storing cryptographic data comprising:

receiving authentication data;

combining the cryptographic data with a first set of bits to form a second set of bits;

combining the cryptographic data with a third set of bits to form a fourth set of bits;

creating a first pairing of the first set of bits with the third set of bits;

creating a second pairing of the first set of bits with the fourth set of bits;

storing one of the first and second pairings in a first computer accessible storage medium; and

storing the other of the first and second pairings in a second computer accessible storage medium.

47. The method of Claim 46, wherein at least one of the first and second computer accessible storage mediums comprises at least one server.

48. The method of Claim 46, wherein the first computer accessible storage medium is geographically remote from the second computer accessible storage medium.

49. The method of Claim 46, wherein the matching of one of the first and second pairings with one of the first and second computer accessible storage mediums is substantially random.

50. The method of Claim 46, wherein at least one of the first and third sets of bits are substantially random.

51. The method of Claim 46, wherein at least one of the first and third sets of bits comprises a bit length equal to a bit length of the sensitive data.

52. The method of Claim 46, wherein both the first and second pairings are needed to reassemble the cryptographic data.

53. The method of Claim 46, further comprising:

creating a third pairing of the second set of bits with the third set of bits;

creating a fourth pairing of the second set of bits with the fourth set of bits;

storing one of the third and fourth pairings in a third computer accessible storage medium; and

storing the other of the third and fourth pairings in a fourth computer accessible storage medium.

54. A method of handling sensitive data in a cryptographic system, wherein the sensitive data exists in a useable form only during actions employing the sensitive data, the method comprising:

receiving in a software module, substantially randomized sensitive data from a first computer accessible storage medium;

receiving in the software module, substantially randomized data from a second computer accessible storage medium,

processing the substantially randomized sensitive data and the substantially randomized data in the software module to assemble the sensitive data; and

employing the sensitive data in a software engine to perform an action, wherein the action includes one of authenticating a user and performing a cryptographic function.

55. The method of Claim 54, further comprising destroying the sensitive data after completion of the action.

56. The method of Claim 54, wherein the sensitive data includes one of user biometric data and cryptographic key data.

57. The method of Claim 54, wherein at least one of the first and second computer accessible storage mediums comprise a secure server.

58. The method of Claim 54, wherein the software module comprises a data assembling module and the software engine comprises one of an authentication engine and a cryptographic engine.

59. A secure authentication system, comprising:

a plurality of authentication engines, wherein each authentication engine receives enrollment authentication data designed to uniquely identify a user to a degree of certainty, each authentication engine receives current authentication data to compare to the enrollment authentication data, and wherein each authentication engine determines an authentication result; and

a redundancy system which receives the authentication result of at least two of the authentication engines and determines whether the user has been uniquely identified.

60. The secure authentication system of Claim 59, wherein the redundancy system determines whether the user has been uniquely identified by following the majority of the authentication results.

61. The secure authentication system of Claim 59, wherein the redundancy system determines whether the user has been uniquely identified by requiring the authentication results to be unanimously positive before issuing a positive identification.

62. The secure authentication system of Claim 59, wherein the redundancy system includes a plurality of redundancy modules, and the secure authentication system further comprises:

a plurality of geographically remote trust engines, each trust engine having one of the plurality of authentication engines and one of the redundancy modules,

wherein the redundancy module for at least one of the plurality of trust engines determines whether the user has been uniquely identified using the authentication results from ones of the authentication engines associated with the other trust engines and without using the authentication results from the at least one trust engine.

63. The secure authentication system of Claim 62, wherein each of the plurality of trust engines includes a depository having a computer accessible storage medium which stores a substantially randomized portion of the enrollment authentication data and wherein each depository forwards the substantially randomized portion of the enrollment authentication data to the plurality of authentication engines.

64. The secure authentication system of Claim 62, wherein the determination of whether the user has been uniquely identified corresponds to the one of the redundancy modules to first determine a result.

65. A trust engine system for facilitating authentication of a user, the trust engine system comprising:

a first trust engine comprising a first depository, wherein the first depository includes a computer accessible storage medium which stores portions of enrollment authentication data;

a second trust engine located at a different geographic location than the first trust engine and comprising

a second depository having a computer accessible storage medium which stores portions of enrollment authentication data,

an authentication engine communicating with the first and second depositories and which assembles at least two portions of enrollment authentication data into a usable form, and

a transaction engine communicating with the first and second depositories and the authentication engine,

wherein when the second trust engine is determined to be available to execute a transaction, the transaction engine receives authentication data from a user and forwards a request for the portions of enrollment authentication data to the first and second depositories, and wherein the authentication engine receives the authentication data from the transaction engine and the portions of the enrollment authentication data from the first and second depositories, and determines an authentication result.

66. The trust engine system of Claim 65, wherein the determination of whether the second trust engine is available to execute the transaction includes a determination of whether the second trust engine is within geographic proximity to the user.

67. The trust engine system of Claim 65, wherein the determination of whether the second trust engine is available to execute the transaction includes a determination of whether the second trust engine is currently servicing a light system load.

68. The trust engine system of Claim 65, wherein the determination of whether the second trust engine is available to execute the transaction includes a determination of whether the second trust engine is currently scheduled for maintenance.

69. The trust engine system of Claim 65, wherein the first and second trust engines are determined to be available, and an authentication result for the trust engine system follows the first of the first and second trust engines to produce the authentication result.